Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 97-213
Communications Assistance for Law Enforcement Act	)	

COMMENTS OF CISCO SYSTEMS, INC.

Scott Blake Harris
Kelly S. McGinn
HARRIS, WILTSHIRE & GRANNIS LLP
1200 Eighteenth Street, N.W.
Washington, D.C. 20036
(202) 730-1300/office
(202) 730-1301/fax

Attorneys for Cisco Systems, Inc.

November 16, 2000

TABLE OF CONTENTS

SUMMARY

Although the September 2001 packet-mode deadline is just ten months away, critical questions abound about what will be required of service providers -- pursuant to CALEA -- when they are served with Title III or pen register/trap and trace orders for packet-mode communications. The D.C. Circuit opinion leaves open the question of which, if any, of the four challenged punch list capabilities carriers will be required to implement. The opinion also leaves packet-mode carriers and equipment manufacturers unsure about what compliance with a pen register order will require given that: (1) *transmitting the entire packet stream has been deemed illegal*; and (2) the exact parameters of "call-identifying information" for packet-mode communications have yet to be clarified. Moreover, before CALEA capability requirements are imposed for packet-mode communications, serious consideration must be given to unique feasibility challenges that may be confronted by service providers cooperating with lawfully authorized intercepts given that packet networks operate very differently from circuit-switched networks.

In light of this uncertainty the Commission must do two things: 1) provide guidance to carriers, manufacturers, law enforcement and the public regarding what compliance with both Title III and pen register requests for packet-mode communications will entail; and 2) suspend the September 2001 compliance deadline until such guidance has been provided and a revised standard for packet-mode communications has been adopted. The alternative is a "gotcha" regime, in which carriers and manufacturers can be punished for failing to meet legal obligations that they cannot understand. Surely Congress and the Commission never intended CALEA to yield such a result.

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 97-213
Communications Assistance for Law Enforcement Act	)	

COMMENTS OF CISCO SYSTEMS, INC.

Cisco Systems, Inc. hereby comments on the August 15, 2000 decision of the United States Court of Appeals for the District of Columbia in *USTA v. FCC*[1], and on related issues associated with the September 2001 CALEA compliance deadline for packet-mode communications.

Although the September 2001 packet-mode deadline is just ten months away, critical questions abound about what will be required of service providers – pursuant to CALEA – when they are served with Title III or pen register/trap and trace orders for packet-mode communications. The D.C. Circuit opinion leaves open the question of which, if any, of the four challenged punch list capabilities carriers will be required to implement. The opinion also leaves packet-mode carriers and equipment manufacturers unsure about what compliance with a pen register order will require given that: (1) ***transmitting the entire packet stream has been deemed illegal***; and (2) the exact parameters of "call-identifying information" for packet-mode communications have yet to be clarified. Moreover, before CALEA capability requirements are imposed for packet-mode communications, serious consideration must be given to unique

[1] United States Telecomm. Ass'n v. F.C.C., No. 99-1442, 2000 U.S. App. LEXIS 19967 (D.C. Cir. Aug. 15, 2000) (*to be reported at* 227 F.3d 450).

feasibility challenges that may be confronted by service providers cooperating with lawfully authorized intercepts given that packet networks operate very differently from circuit-switched networks.

In light of this uncertainty the Commission must do two things: 1) provide guidance to carriers, manufacturers, law enforcement and the public regarding what compliance with both Title III and pen register requests for packet-mode communications will entail; and 2) suspend the September 2001 compliance deadline until such guidance has been provided and a revised standard for packet-mode communications has been adopted. The alternative is a "gotcha" regime, in which carriers and manufacturers can be punished for failing to meet legal obligations that they cannot understand. Surely Congress and the Commission never intended CALEA to yield such a result.

BACKGROUND

CALEA was enacted in 1994 as a reasoned response to the impact that new technologies were having on the ability of law enforcement agencies to conduct lawful electronic surveillance. Over the past six years, advances in communications technologies have not slowed – and these advances did not inform the crafting of CALEA's definitional language and service requirements. Nor, of course, were they taken into account by the J-STD-025 standard ("J-Standard"), one of the safe harbor standards developed by the industry, for compliance with packet-mode intercept requests. Internet telephony ("Voice over IP" or "VoIP") is only one example of such a technology. Yet, as the September 2001 CALEA deadline for packet-mode communications approaches, packet-mode service providers and equipment manufacturers have no clear statement of requirements for purposes of preparing to implement intercepts. In its 1999 *Third Report and Order*, the Commission candidly acknowledged that the proceeding did not "sufficiently address

packet technologies and the problems that they may present for CALEA purposes."[2] Although the primary concern at the time was the technical and privacy concerns associated with separating call-identifying information from call content in response to a pen register order, the Commission tacitly acknowledged that a "one-size-fits-all" solution might not be possible for packet-mode intercepts given the tremendous variation in the processing of communications by packet-mode technologies.[3]

As a result, the Commission invited TIA to study CALEA solutions for packet-mode technology and to report on steps that could be taken to improve the J-Standard, particularly with respect to the protection of privacy. Despite a great deal of work by the Telecommunications Industry Association ("TIA"), culminating in the release of the September 29, 2000 *Report on Surveillance of Packet-mode Technologies* ("the Joint Experts Meeting Report" or "JEM Report"), a revised standard for packet-mode communications does not yet exist.

The results of TIA's work will, of course, inform the revision process. The JEM report acknowledges that, given the wide array of technologies that have been developed, one packet-mode standard may not be sufficient for all protocols.

In addition to the challenge of considering how to devise a "one size fits all solution" for differing packet-mode protocols, TIA found its efforts to improve the J-Standard stymied by CALEA's lack of definitional clarity and by other technical challenges unique to packet-mode

---

[2] In the Matter of Communications Assistance for Law Enforcement Act, *Third Report & Order*, 14 F.C.C. Rcd. 16794, 16819, ¶ 55 (rel. Aug. 31, 1999).

[3] The *Third Report and Order* specifically noted that "some packet technologies (e.g., frame relay, ATM, X.25) are connection oriented –*i.e*., there are call set-up and take-down processes, similar to those in circuit-switched voice networks, whereby addressing information is made available separate from and before call content is transmitted. Other packet technologies (*e.g*., internet protocol-based solutions) would not be processed this way." *Id at* ¶ 55.

communications. Specifically, the JEM contributors noted that "based on current FCC guidance, it could not define 'call-identifying information' for packet services."[4] Second, they noted that although CALEA requirements apply to telecommunications service and not information services, "from a packet point of view, the two may be indistinguishable."[5] Indeed, they concluded that "it is not technically advisable to determine on a packet-by-packet basis, the application or communications services that is being provided" and that "the possibility of encapsulation or encryption of packets outside of the service provider's control makes identifying the application or service even more unlikely."[6]

Thus, as recommended by TIA upon transmittal of the JEM Report to the Commission and made necessary by the D.C. Circuit opinion in *USTA v. FCC*, the Commission should suspend the September 2001 packet-mode CALEA deadline in favor of a serious review of the unique implementation challenges that apply to packet-mode intercepts, and the establishment of a set of prescriptions that resolve ambiguities about the application of CALEA to packet-mode communications. If CALEA is to work, the obligations of industry must be workable. Today they are not.

---

4 Telecommunication Industry Association, *Report to the Federal Communications Commission on Surveillance of Packet-Mode Technologies* 10 (Sept. 29, 2000)(hereinafter "JEM Report").

5 *Id.*

6 *Id.*

I. THE COMMISSION IS REQUIRED TO SUSPEND THE SEPTEMBER 2001 PACKET-MODE DEADLINE.

CALEA mandates that the Commission take five factors into account when reviewing allegedly deficient technical requirements or standards.[7] Following the D.C. Circuit's remand in *USTA v. FCC,* the Commission is now collecting information to ensure the satisfaction of the first two of these factors: 1) that the standard meets the assistance capability requirements by cost-effective methods; and 2) that the standard protects the privacy and security of communications not authorized to be intercepted.[8] During this review, the Commission is obligated to suspend the September 2001 compliance deadline based on the fifth of these factors: that the Commission provide ***reasonable time and conditions for compliance with and the transition to any new standard.***[9] The D.C. Circuit's decision has created significant uncertainty with respect to the capabilities that carriers must implement on September 2001, and renders it impossible for manufacturers to support carriers with appropriate equipment until the Commission offers clear guidance.

In the *Third Report and Order* the Commission charged the telecommunications industry with implementing six additional capability requirements – the "punch list" – by September 2001. TIA prepared a revised J-Standard to incorporate all six functionalities. However, the D.C. Circuit vacated and remanded those provisions of the *Third Report and Order* dealing with four of the punch list items. Nonetheless, carriers currently remain subject to the September 2001 compliance deadline for the two punch list items that were not challenged in the case – timing and conference call content delivery. Thus, neither the J-Standard nor the revised J-Standard

---

7 *See* 47 U.S.C. 1006(b).

8 47 U.S.C. § 1006(b)(1)-(2).

9 47 U.S.C. § 1006(b)(5).

accurately reflects the capability requirements that will ultimately be required of carriers once the Commission has completed its review of the punch list items remanded by the D.C. Circuit.

Similarly, in the *Third Report and Order* the Commission required carriers to comply with the J-Standard for packet-mode communications as of September 2001 – notwithstanding the fact that "under this standard, law enforcement agencies would be provided with both call-identifying information and call content ***even in cases where a LEA is authorized only to receive call-identifying information*** (i.e., under a pen register)."[10] The Commission simultaneously charged the industry with consulting on a permanent solution that would resolve privacy concerns by September 2000, and to prepare to implement the existing J-Standard as a temporary remedy by September 2001. In its decision, however, the D.C. Circuit rejected the Commission's conclusion that it was permissible for law enforcement agencies to obtain the *contents* of communications (i.e. the entire packet stream) in response to an order limited to provision of call-identifying information. Thus, the court held that carriers relying on the interim J-Standard who provide the entire packet stream in response to a pen register order would be committing an illegal act:

> All of CALEA's required capabilities are expressly premised on the condition that any information will be obtained "pursuant to court order or other lawful authorization." 47 U.S.C. § 1002(a)(1)-(3). ***CALEA authorizes neither the Commission nor the telecommunications industry to modify either the evidentiary standards or procedural safeguards for securing legal authorization*** to obtain packets from which call content has not been stripped, ***nor may the Commission require carriers to provide the government with information that is not authorized to be intercepted."***[11]

---

[10] *Third Report and Order*, 14 F.C.C. Rcd. at 16819, ¶55.

[11] *United States Telecom Ass'n v. F.C.C.*, 2000 U.S. App. LEXIS 19967, at *44 (emphasis supplied).

In light of this ruling, it is plainly unreasonable to demand that equipment manufacturers and carriers implement the J-Standard in September 2001 – and risk violating the law. The J-Standard, after all, is supposed to be a ***safe*** harbor.

Before CALEA can be implemented for packet-mode communications – at a minimum – equipment will need to be redesigned to ensure call-identifying information can be segregated from content before delivery to law enforcement. Packet equipment will also need to be updated to be capable of implementing the punch list items that the Commission ultimately rules must be provided. More significant equipment changes may also be necessary based on the Commission's review of the JEM Report. Thus, the Commission should allow the packet-mode communications industry to focus its efforts on cooperating in the revision of current standards, rather than preparing to comply with a standard that does not protect the privacy and security of communications.

II. THE FCC SHOULD DEFINE "CALL-IDENTIFYING INFORMATION" FOR IP PACKET-MODE COMMUNICATIONS AS SOURCE AND DESTINATION IP ADDRESSES AND CALLED AND CALLING PARTY NUMBERS.

CALEA requires carriers to be capable of providing the government with call-identifying information in a manner that protects both the privacy of communications and call-identifying information not authorized to be intercepted.[12] Recognizing that the J-Standard did not fully comply with this requirement, the Commission charged TIA with studying ways in which the standard could be revised better to protect privacy. It is, thus, noteworthy that the JEM Report noted that, due to a lack of guidance, "it could only attempt to identify what information may be

[12] *See* 47 U.S.C. §1002(4)(A).

available about the packet communication without regard to whether it might be characterized as 'call-identifying information' under CALEA."[13]

CALEA defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communications generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[14] This definition implicitly assumes circuit-switched technology, and the common use of pen register or trap and trace devices for circuit-switched communication. Pen registers record the telephone number to which calls have been placed from a particular telephone. Trap and trace devices record the numbers of telephones from which calls have been placed to a particular telephone. But in IP packet-mode communications there may be no telephone numbers to be recorded by a pen register or a trap and trace device. It is critical that a workable definition of call-identifying be agreed upon for packet-mode communications because of its constitutional significance: call content is protected by the Fourth Amendment but call identifying information, at least as it has been understood traditionally (i.e., telephone numbers), is not.[15] The Commission must therefore determine what type of packet-mode data is akin to a phone number, and can be provided to law enforcement without also revealing content.

Although there is no packet-mode analogue to telephone numbers, Cisco believes the best way to way to define call identifying information in the IP packet-mode context is the Internet Protocol source and destination addresses associated with the communication (and, if available, the called and calling telephone numbers). Source and destination IP addresses are akin to

---

[13] JEM Report at 10.

[14] 47 U.S.C. § 1001(2).

[15] *See Smith v. Maryland, 442 U.S. 735, 742-45 (1979).*

telephone numbers in that they identify the IP network end-points of a call. Requiring the provision of additional information, such as email addresses, would require the examination of other "layers" of protocol that belong to the application, not the packet transport. This is both expensive and involves the examination of information that is clearly content.

III. THE COMMISSION SHOULD NOT REQUIRE IMPLEMENTATION OF THE FOUR REMANDED PUNCH LIST ITEMS.

Cisco urges the Commission not to require implementation of the four remanded punch list items for IP packet-mode communications. Because these features are implemented differently in IP packet-mode networks than in circuit-switched networks, some of these items are not feasible to implement, while others would require adding expensive filtering functionality. Some punch list features are not implemented the same way in all packet-mode protocols, or in all packet-mode end-user products. Consequently, it is important to consider individually various proposed features associated with the punch list items to determine whether it is feasible to implement them in IP packet-mode networks and, if so, whether this can be done on a cost-effective basis. Where different networks implement punch list items in different ways, the cost of implementing these items under CALEA skyrockets.

To cite some examples of the problems that might arise with implementation of the punch list items on IP packet-mode networks, consider the case of "post-cut-through dialed digit extraction." On IP networks, these additional digits are carried in the same type of packets that contain voice content. The dialed digit information is not seen by the call management service in the same way that other "call events" are and cannot be extracted in the same manner as an IP address. To extract this information for law enforcement, routers would have to perform filtering operations within the application layer of the IP packet content – a difficult and expensive task at best. Even then, it is possible that such "dialed digits" might be contained in a protocol that the

routers would not recognize. In any case, such filtering would surely result in performance degradation as well as exorbitant cost.

In the case of "party hold/join/drop information," there are limits to the provision of this type of information based on the way in which packet networks route voice communications. For example, certain functions such as "call hold" are performed by the end user devices and do not involve any "call event" messages sent to the network equipment. In the case of multi-party calls (involving "joins" and "drops"), a service provider's equipment can only see packets and call events relating to subscribers on its network that are still a part of a multi-party call.

For example, suppose a target, X, is a subscriber to Service Provider A's network. Suppose further that target X establishes an IP call with Y and Z, and neither Y nor Z is a subscriber to service provider A's network. If target X "hangs up" on the call, but correspondents Y and Z continue to communicate, then service provider A will no longer have any connection to the packets containing the communication between Y and Z, nor to any call events associated with that call.

The cost and feasibility of providing "subject-initiated dialing and signaling information" and "in-band" and "out-of-band signaling" features must be addressed on a feature by feature basis. In general, the terms "signaling," "in-band," and "out-of-band" do not translate directly from the circuit-switched environment to the IP packet-mode environment. Moreover, this is the area where there is the highest degree of variability depending upon which VoIP protocol is used. Furthermore, it is inappropriate to simply designate that all information exchanged between an end-user's device and the CMS should be classified as "signaling information" and required to be made available to the law enforcement agency in that guise. Each of these four "punch list" requirements adds incremental cost to the adherence to CALEA regulations. More detailed

identification of the desired features is necessary to analyze how much complexity and cost will be incurred to provide these items. In the absence of cost-justified arguments to include these capabilities, we urge the Commission to omit them from the regulations for the present. CALEA implementation in IP networks will simply work better if the Commission makes sure that the basic intercept capabilities are met, and does not require gold-plated technology that disproportionately increases implementation costs while offering no guarantees that the information sought can always be made available.

IV. THE FCC SHOULD CONSIDER FEASIBILITY CHALLENGES UNIQUE TO IP PACKET-MODE NETWORKS BEFORE SETTING A PACKET-MODE DEADLINE.

Before imposing a final CALEA capability compliance deadline for packet-mode communications, Cisco urges the Commission to consider the unique challenges presented for conducting intercepts on IP packet networks as compared with circuit-switched networks. When conducting intercepts on traditional circuit-switched networks, law enforcement approaches one carrier to provide access to a stream of communications to or from the intercept subject. This may not be possible with an IP network. All VoIP involves at least two separable functions: "call management" and voice transport. A call management service ("CMS") is the set of functions that determine how a call is routed and what features apply while the call is in progress. Voice transport in an IP packet network involves the packetization and carriage of digitized voice inside the IP protocol. In traditional circuit-switched networks the call management function and the voice transport function are virtually always implemented together in a single switching device. In VoIP, however, these functions may be and often are separated. Indeed, the ***call management and voice transport components of a VoIP call may be handled by different service providers***. In such a case it may be impossible for either provider to assemble all of the information necessary

to intercept a VoIP "call." The service provider offering the transport layer of the communication will in effect simply be supplying the pipe through which the packets pass. The entity providing the call management software at its gateway never possesses the content of the packet stream and, therefore, would be incapable of intercepting it. An interception in this case would thus only be possible if the same service provider provided both the transport and call management components of the VoIP "call."

For example, if a target begins a VoIP "call" from a PC, his ISP typically processes only the IP protocol header. The ISP's network is otherwise unaware that a voice communication is being started. As the JEM Report noted:

> Routers supporting service on the Internet typically only make routing decisions based on the IP addressing information. Service providing equipment is not generally designed to look past the IP headers (some may look at TCP or UDP port numbers for filtering) when switching or routing packets. Any processing capacity used for extracting information from a packet stream is, thus, not available for routing packets. Given the increase in capacity of Internet connections and that systems generally run at peak load much of the time, there is very little capacity to monitor data fields.[16]

Increasing the capacity of the router to be able to perform this intense filtering operation so that it can look into the application layer of every packet to determine when a target's device is communicating with an outside CMS would be an extremely expensive proposition and would require massive upgrades of existing packet network equipment.

Moreover, adding such functionally would cut performance of a router significantly and seriously degrade the functioning of high-speed networks.

Another theoretical possibility would be to put the burden for detecting VoIP "calls" not on the ISP, but on the provider of the CMS. However, since, like the World Wide Web, virtually

---

[16] JEM Report at 58.

anyone could start a business providing CMS functionality, and the target could choose any such business as a means of making a VoIP "call," trying to track a particular target would mean court orders addressed to hundreds or thousands of potential CMS providers. Since the Internet is a global network, there will be CMS's that are located outside the United States and therefore are beyond the reach of the U.S. legal system.

Even if it were feasible to issue intercept orders to large numbers of CMS providers, the information that could be provided by such providers would be limited to "call-identifying information" as defined in Section II of these comments. The CMS provider would not be able to provide call content in the case of a Title III order, since the actual voice packets would not likely traverse the CMS or any other device of the CMS provider. Similar caveats must be recognized in the case of end-users accessing VoIP services in conjunction with mobile wireless access. A service provider may provide VoIP (including both packet transport and the CMS) but not provide the actual mobile wireless service over which the service is delivered. In this case, the VoIP service provider does not necessarily have access to the antenna location. If a service provider is providing only a CMS, but not packet transport then it may not have access to antenna location information. In fact, the service provider may not even know that wireless technology is being used in the access network. In these cases the VoIP service provider will not be able to provide location information beyond the phone numbers and IP addresses used for the call. If the VoIP CMS is tightly integrated into the wireless infrastructure, then antenna location information may be available. This variability in availability of location information in the case of IP networks must be accounted for in the final version of the CALEA regulations.

The bottom line is that IP networks do not look or act like circuit-switched networks. Many assumptions about what circuit-switched carriers can do to intercept calls simply do not

apply to IP service providers. Equipment manufacturers, carriers, law enforcement and the public will be served far better by the resolution of the technical uncertainty that currently exists with respect to how to implement CALEA for packet-mode communications, than by slavishly rushing toward an implementation deadline with which it is currently impossible to comply.

CONCLUSION

Cisco respectfully requests that the Commission extend the September 2001 implementation deadline for packet-mode communications in light of the ongoing Commission review of the J-Standard prompted by the D.C. Circuit opinion in *USTA v. FCC*, as well as the significant technological ambiguity that currently exists with respect to applying CALEA to real-world packet-mode intercepts.

Respectfully submitted,

CISCO SYSTEMS, INC.

By: /s/ Scott Blake Harris
Scott Blake Harris
Kelly S. McGinn
HARRIS, WILTSHIRE & GRANNIS LLP
1200 Eighteenth Street, N.W.
Washington, D.C. 20036
(202) 730-1300/office
(202) 730-1301/fax

November 16, 2000

Attorneys for Cisco Systems, Inc.